11.3 NAT, PAT und Portweiterleitung im Detail

NAT und PAT werden in IPv4-Netzwerken sehr häufig eingesetzt.

Sie ermöglichen, dass interne private IP-Adressen mit externen Netzen kommunizieren können.

NAT steht für:

```
Network Address Translation
```

PAT steht für:

```
Port Address Translation
```

Portweiterleitung wird genutzt, um einen internen Dienst von außen erreichbar zu machen.

Merksatz:

```
NAT übersetzt IP-Adressen.
PAT übersetzt IP-Adressen und Ports.
Portweiterleitung macht interne Dienste erreichbar.
```

Warum gibt es NAT?

IPv4-Adressen sind begrenzt.

Deshalb werden in lokalen Netzwerken häufig private IPv4-Adressen verwendet.

Diese privaten Adressen sind im Internet nicht direkt geroutet.

Beispiele:

```
192.168.1.10
10.0.0.20
172.16.5.30
```

Damit solche Geräte trotzdem ins Internet können, übersetzt ein Router oder eine Firewall die privaten Adressen in eine öffentliche Adresse.

Merksatz:

NAT ermöglicht Internetzugang mit privaten IPv4-Adressen.

Private IPv4-Adressen

Private IPv4-Adressbereiche sind für interne Netze vorgesehen.

Bereich	CIDR	typische Nutzung
10.0.0.0 bis 10.255.255.255	10.0.0.0/8	große interne Netze
172.16.0.0 bis 172.31.255.255	172.16.0.0/12	mittlere interne Netze
192.168.0.0 bis 192.168.255.255	192.168.0.0/16	Heimnetze und kleine Netze

Diese Adressen sind im öffentlichen Internet nicht direkt erreichbar.

Merksatz:

Private IPv4-Adressen sind intern nutzbar,
aber nicht öffentlich geroutet.

Öffentliche IPv4-Adresse

Eine öffentliche IPv4-Adresse ist im Internet routbar.

Sie wird zum Beispiel vom Internetanbieter zugewiesen.

Beispiel:

Router WAN-Adresse:
öffentliche IPv4-Adresse

Client im LAN:
private IPv4-Adresse

Der Router übersetzt beim Internetzugriff die private Adresse in die öffentliche Adresse.

Merksatz:

Öffentliche IP-Adresse ist im Internet sichtbar.

NAT-Grundprinzip

Ein interner Client baut eine Verbindung ins Internet auf.

Vor NAT:

```
Quelle:
192.168.10.50

Ziel:
93.184.216.34
```

Nach NAT:

```
Quelle:
öffentliche IP des Routers

Ziel:
93.184.216.34
```

Der externe Server sieht nicht die private IP des Clients, sondern die öffentliche IP der Firewall oder des Routers.

Merksatz:

```
NAT versteckt private Quelladressen hinter einer öffentlichen Adresse.
```

NAT-Tabelle

Damit Antworten wieder zum richtigen internen Client zurückkommen, führt das NAT-Gerät eine Zuordnungstabelle.

Dort steht vereinfacht:

```
Interner Client mit internem Port
gehört zu
externer Verbindung mit übersetztem Port.
```

Beispiel:

intern	extern sichtbar	Ziel
192.168.10.50:50123	203.0.113.10:61001	93.184.216.34:443
192.168.10.51:50200	203.0.113.10:61002	93.184.216.34:443

Merksatz:

> NAT merkt sich,
> welche interne Verbindung zu welcher externen Verbindung gehört.

Source NAT

Source NAT ändert die Quelladresse.

Typischer Fall:

> interner Client geht ins Internet.

Vor Source NAT:

> Quelle:
> 192.168.10.50
>
> Ziel:
> 93.184.216.34

Nach Source NAT:

> Quelle:
> öffentliche IP
>
> Ziel:
> 93.184.216.34

Merksatz:

> Source NAT ändert die Quelle.

Destination NAT

Destination NAT ändert die Zieladresse.

Typischer Fall:

```
externer Zugriff auf internen Dienst.
```

Beispiel:

```
öffentliche IP TCP 443
wird weitergeleitet an
interner Webserver TCP 443
```

Vor Destination NAT:

```
Ziel:
öffentliche IP:443
```

Nach Destination NAT:

```
Ziel:
192.168.10.20:443
```

Merksatz:

```
Destination NAT ändert das Ziel.
```

PAT

PAT steht für:

```
Port Address Translation
```

PAT übersetzt zusätzlich Ports.

Das ist besonders wichtig, wenn viele interne Geräte dieselbe öffentliche IPv4-Adresse verwenden.

Beispiel:

Client A:

192.168.10.10:50001

Client B:

192.168.10.11:50001

Extern kann beides über dieselbe öffentliche IP laufen, weil unterschiedliche übersetzte Ports genutzt werden.

Merksatz:

PAT macht viele interne Verbindungen über eine öffentliche IP möglich.

NAT und PAT vergleichen

Begriff	Bedeutung	Beispiel
NAT	IP-Adresse wird übersetzt	192.168.10.50 → öffentliche IP
PAT	IP-Adresse und Port werden übersetzt	192.168.10.50:50123 → öffentliche IP:61001
Source NAT	Quelle wird geändert	LAN → Internet
Destination NAT	Ziel wird geändert	Internet → interner Server
Portweiterleitung	externer Port wird intern weitergeleitet	WAN:443 → Server:443

Merksatz:

NAT = Adresse.

PAT = Adresse plus Port.

Warum PAT so häufig ist

In Heimnetzen und kleinen Unternehmensnetzen gibt es oft nur eine öffentliche IPv4-Adresse.

Trotzdem sollen viele Geräte gleichzeitig ins Internet.

Beispiele:

```
Notebook
Smartphone
Server
Drucker
Smart-TV
NAS
virtuelle Maschinen
```

PAT unterscheidet diese Verbindungen über Ports.

Merksatz:

```
PAT löst das Problem,
dass viele interne Geräte eine öffentliche IPv4-Adresse teilen.
```

Portweiterleitung

Portweiterleitung bedeutet:

```
Ein Port auf der öffentlichen Adresse wird an ein internes Ziel weitergeleitet.
```

Beispiel:

```
öffentliche IP:443
→ 192.168.10.20:443
```

Oder:

```
öffentliche IP:8443
→ 192.168.10.20:443
```

Portweiterleitung ist eine Form von Destination NAT.

Merksatz:

```
Portweiterleitung leitet externe Anfragen an interne Dienste weiter.
```

Beispiel: Webserver intern veröffentlichen

Situation:

```
Interner Webserver:
192.168.10.20

Dienst:
HTTPS TCP 443
```

Ziel:

```
Benutzer aus dem Internet sollen den Webserver erreichen.
```

Benötigt:

```
DNS zeigt auf öffentliche IP.
Portweiterleitung WAN:443 → 192.168.10.20:443.
Firewall-Regel erlaubt TCP 443.
Webserver hört auf TCP 443.
Zertifikat passt zum Hostnamen.
```

Merksatz:

```
Externer Webzugriff braucht DNS,
NAT,
Firewall,
Dienst
und Zertifikat.
```

Portweiterleitung und Firewall-Regel

Eine Portweiterleitung allein reicht nicht immer.

Man braucht oft zusätzlich eine Firewall-Regel.

NAT-Regel:

```
Wohin soll der Verkehr übersetzt werden?
```

Firewall-Regel:

```
Darf der Verkehr überhaupt durch?
```

Beispiel:

```
NAT:
WAN:443 → Webserver:443

Firewall:
Erlaube WAN → Webserver TCP 443
```

Wenn die Firewall blockiert, funktioniert der Zugriff trotz NAT nicht.

Merksatz:

```
NAT leitet um.
Firewall erlaubt oder blockiert.
```

Portweiterleitung und DNS

Damit Benutzer einen Dienst bequem erreichen, wird meist ein DNS-Name genutzt.

Beispiel:

```
cloud.firma.de
→ öffentliche IP
```

Dann leitet die Firewall weiter:

```
öffentliche IP:443
→ interner Server:443
```

Wenn DNS auf die falsche IP zeigt, erreicht der Benutzer den falschen Anschluss oder Server.

Merksatz:

```
DNS muss zur öffentlichen Adresse der Portweiterleitung passen.
```

Portweiterleitung und Zertifikate

Bei HTTPS muss das Zertifikat zum aufgerufenen Namen passen.

Beispiel:

```
Benutzer ruft auf:
https://cloud.firma.de
```

Zertifikat muss gültig sein für:

```
cloud.firma.de
```

Wenn DNS oder Portweiterleitung auf den falschen Server zeigt, kann ein falsches Zertifikat ausgeliefert werden.

Merksatz:

```
HTTPS-Veröffentlichung braucht passenden DNS-Namen und passendes Zertifikat.
```

Portweiterleitung und Reverse Proxy

Oft wird nicht jeder interne Dienst direkt veröffentlicht.

Stattdessen zeigt die Portweiterleitung auf einen Reverse Proxy.

Beispiel:

```
öffentliche IP:443
→ Reverse Proxy in DMZ
```

Der Reverse Proxy leitet dann nach Hostname weiter:

```
wiki.firma.de → interner Wiki-Server
cloud.firma.de → interner Cloud-Server
git.firma.de → interner Git-Server
```

Merksatz:

Reverse Proxy kann mehrere interne Webdienste über HTTPS bündeln.

Portweiterleitung und mehrere Dienste

Ein öffentlicher Port kann auf einer öffentlichen IP nur einmal eindeutig belegt werden.

Beispiel:

öffentliche IP:443
kann nicht gleichzeitig direkt auf drei verschiedene Server zeigen.

Lösung:

Reverse Proxy mit Hostnamen
oder
unterschiedliche externe Ports
oder
mehrere öffentliche IP-Adressen

Merksatz:

Ein Port auf einer IP kann nur eindeutig einem Ziel zugeordnet werden.

Externer Port und interner Port

Bei Portweiterleitung können externer und interner Port gleich oder unterschiedlich sein.

Beispiel gleich:

WAN:443 → Server:443

Beispiel unterschiedlich:

WAN:8443 → Server:443

Das kann für Tests nützlich sein, sollte aber sauber dokumentiert werden.

Merksatz:

Externer Port und interner Port müssen nicht identisch sein.

Sicherheitsrisiko Portweiterleitung

Eine Portweiterleitung macht einen internen Dienst von außen erreichbar.

Das erhöht die Angriffsfläche.

Risiken:

- Brute-Force-Angriffe
- Ausnutzung von Schwachstellen
- Fehlkonfiguration
- veraltete Software
- offene Adminoberflächen
- schwache Passwörter
- unnötige Dienste im Internet

Merksatz:

Jeder veröffentlichte Port ist ein potenzieller Angriffspunkt.

Was sollte man nicht direkt veröffentlichen?

Nicht direkt ins Internet gehören normalerweise:

- SMB TCP 445
- RDP TCP 3389
- Datenbankports
- Drucker
- interne Adminoberflächen
- Hypervisor-Management
- NAS-Adminoberflächen
- unsichere Webinterfaces
- Telnet TCP 23
- unverschlüsseltes FTP

Besser:

VPN,
Reverse Proxy,
Zero-Trust-Zugriff,
Bastion Host
oder
gezielte Zugriffsbeschränkung.

Merksatz:

Administrative und interne Dienste nicht direkt ins Internet öffnen.

Portweiterleitung und Quellbeschränkung

Eine Portweiterleitung kann sicherer werden, wenn nur bestimmte Quellen erlaubt sind.

Beispiel:

Nur Admin-IP darf SSH erreichen.

Oder:

Nur Partnernetz darf API erreichen.

Vorteil:

nicht jeder im Internet kann den Dienst erreichen.

Merksatz:

Wenn möglich,
Zugriff auf bekannte Quellen beschränken.

Portweiterleitung und VPN

Oft ist VPN sicherer als direkte Portweiterleitung.

Beispiel:

```
Kein RDP direkt aus dem Internet.
```

Stattdessen:

```
Benutzer verbindet sich per VPN.
Danach RDP intern nutzen.
```

Vorteil:

```
RDP-Port ist nicht öffentlich sichtbar.
```

Merksatz:

```
Für Administration lieber VPN statt direkter Portweiterleitung.
```

NAT ist keine echte Sicherheitsfunktion

NAT verhindert zwar, dass interne private Adressen direkt aus dem Internet erreichbar sind.

Aber NAT ist nicht dasselbe wie eine Firewall.

Eine Firewall prüft und steuert Verkehr bewusst.

NAT übersetzt Adressen.

Merksatz:

```
NAT ist nicht automatisch Sicherheit.
```

NAT und IPv6

Bei IPv6 ist NAT normalerweise nicht in derselben Form nötig, weil es sehr viele öffentliche IPv6-Adressen gibt.

IPv6-Netze arbeiten eher mit:

```
- Routing
- Firewall-Regeln
```

- global eindeutigen Adressen
- Prefix Delegation

Wichtig:

Ohne NAT sind Systeme nicht automatisch ungeschützt.
Die Firewall bleibt entscheidend.

Merksatz:

IPv6 braucht meist weniger NAT,
aber weiterhin Firewall-Regeln.

NAT und Protokollprobleme

Manche Protokolle sind schwierig mit NAT.

Gründe:

- IP-Adressen stehen im Protokollinhalt
- mehrere Verbindungen werden verwendet
- dynamische Ports werden genutzt
- eingehende Rückverbindungen sind nötig

Beispiele:

FTP
SIP
bestimmte VPN-Protokolle
ältere Anwendungen

Merksatz:

NAT kann Protokolle stören,
die zusätzliche Verbindungsinformationen enthalten.

FTP und NAT

FTP kann mit NAT kompliziert sein, weil FTP Steuer- und Datenverbindungen verwendet.

Typische Fehler:

```
Login funktioniert,
aber Dateiliste nicht.
Dateiübertragung startet nicht.
Passiver Portbereich ist nicht freigegeben.
Server gibt falsche externe IP aus.
```

Merksatz:

```
FTP braucht bei NAT besondere Beachtung.
```

SIP und NAT

SIP wird häufig bei VoIP verwendet.

SIP kann durch NAT Probleme bekommen, weil Adressen und Ports im Signalisierungsverkehr eine Rolle spielen.

Mögliche Fehler:

```
kein Audio
nur einseitiges Audio
Anrufaufbau scheitert
Registrierung bricht ab
```

Merksatz:

```
VoIP-Protokolle können durch NAT besondere Probleme bekommen.
```

NAT Loopback

NAT Loopback ist ein anderer Begriff für Hairpin NAT.

Es beschreibt, dass interne Clients über die öffentliche Adresse auf einen internen Dienst zugreifen.

Beispiel:

```
Client im LAN ruft cloud.firma.de auf.
DNS liefert öffentliche IP.
Router leitet Verbindung wieder zurück nach innen.
```

Merksatz:

```
NAT Loopback = Hairpin NAT.
```

Hairpin NAT

Hairpin NAT bedeutet:

```
Ein interner Client nutzt die öffentliche Adresse,
um einen internen Dienst zu erreichen.
```

Ohne Hairpin NAT kann passieren:

```
Dienst funktioniert extern,
aber intern über denselben Namen nicht.
```

Alternative:

```
Split DNS
```

Merksatz:

```
Hairpin NAT hilft,
wenn interne Clients öffentliche Namen verwenden.
```

Split DNS

Split DNS liefert intern und extern unterschiedliche DNS-Antworten.

Beispiel:

```
cloud.firma.de extern:
öffentliche IP

cloud.firma.de intern:
interne IP
```

Vorteil:

```
interne Clients gehen direkt zum internen Ziel,
ohne Hairpin NAT zu brauchen.
```

Merksatz:

```
Split DNS ist oft sauberer als Hairpin NAT.
```

CGNAT

CGNAT steht für:

```
Carrier Grade NAT
```

Dabei teilt der Provider eine öffentliche IPv4-Adresse auf mehrere Kunden auf.

Der eigene Router bekommt dann keine echte öffentliche IPv4-Adresse.

Folge:

```
klassische eingehende Portweiterleitungen funktionieren oft nicht.
```

Erkennbar oft daran:

```
WAN-IP am Router ist privat oder aus speziellem Providerbereich,
aber öffentliche IP im Internet ist eine andere.
```

Merksatz:

```
CGNAT verhindert häufig direkte eingehende IPv4-Verbindungen.
```

Lösungen bei CGNAT

Wenn eingehende Verbindungen wegen CGNAT nicht funktionieren, gibt es mögliche Alternativen:

- echte öffentliche IPv4-Adresse beim Provider buchen
- IPv6 verwenden
- VPN zu einem externen Server
- Cloud-Tunnel
- Reverse SSH Tunnel
- Zero-Trust-Tunnel
- Hosting eines öffentlichen Einstiegspunkts

Merksatz:

Bei CGNAT braucht man oft Tunnel,
IPv6
oder eine echte öffentliche IPv4-Adresse.

Double NAT

Double NAT bedeutet:

Es gibt zwei NAT-Geräte hintereinander.

Beispiel:

Provider-Router macht NAT.
Eigener Router macht ebenfalls NAT.

Folgen:

- Portweiterleitungen müssen auf beiden Geräten passen
- Fehlersuche wird schwieriger
- manche Protokolle machen Probleme
- Gaming, VPN oder VoIP können gestört sein

Merksatz:

Double NAT erschwert eingehende Verbindungen.

NAT und Rückweg

Damit NAT funktioniert, muss der Rückverkehr wieder über dasselbe NAT-Gerät laufen.

Wenn Rückwege anders laufen, kann die Zuordnung fehlen.

Das betrifft besonders:

- mehrere Router
- mehrere Firewalls
- asymmetrisches Routing
- mehrere Internetanschlüsse
- komplexe VPN-Setups

Merksatz:

NAT braucht passenden Rückweg.

Portweiterleitung testen

Beim Testen einer Portweiterleitung sollte man prüfen:

DNS zeigt auf richtige öffentliche IP?
öffentliche IP ist wirklich am Anschluss?
CGNAT ausgeschlossen?
NAT-Regel korrekt?
Firewall-Regel korrekt?
Zielserver erreichbar?
Dienst läuft auf Zielport?
Zielserver-Firewall erlaubt Zugriff?
Zertifikat passt?
Logs zeigen Verbindungsversuch?

Merksatz:

Portweiterleitung braucht mehrere passende Bausteine.

Typisches Fehlerbild: Portweiterleitung funktioniert nicht

Mögliche Ursachen:

```
- falsche öffentliche IP
- CGNAT
- Double NAT
- Portweiterleitung auf falsches Ziel
- falscher interner Port
- Firewall-Regel fehlt
- Dienst läuft nicht
- Host-Firewall blockiert
- DNS zeigt falsch
- Provider blockiert Port
- Test aus internem Netz ohne Hairpin NAT
- Zertifikatsproblem bei HTTPS
```

Merksatz:

```
Portweiterleitungsfehler sind oft NAT-,
Firewall-,
DNS-
oder Dienstprobleme.
```

Fehlerbild: Von außen geht es, von innen nicht

Mögliche Ursachen:

```
- Hairpin NAT fehlt
- internes DNS zeigt falsch
- Split DNS fehlt
- interne Firewall blockiert
- Zertifikat passt intern nicht
- interner Client nutzt anderen Pfad
```

Lösungsideen:

Split DNS einrichten
oder
Hairpin NAT aktivieren

Merksatz:

Extern funktioniert,
intern nicht:
Hairpin NAT oder Split DNS prüfen.

Fehlerbild: Von innen geht es, von außen nicht

Mögliche Ursachen:

- NAT-Regel fehlt
- Firewall-Regel fehlt
- externe DNS-Antwort falsch
- Dienst nur intern gebunden
- öffentliche IP falsch
- Provider blockiert
- CGNAT
- Zertifikat oder Reverse Proxy falsch
- Zielserver-Firewall blockiert

Merksatz:

Intern funktioniert,
extern nicht:
öffentliche Erreichbarkeit prüfen.

Fehlerbild: Falscher interner Dienst antwortet

Mögliche Ursachen:

- Portweiterleitung zeigt auf falschen Host
- Reverse Proxy leitet falsch weiter
- DNS zeigt auf falsche IP

- Host-Header passt nicht
- falscher virtueller Host
- alte NAT-Regel greift vorher
- Regelreihenfolge falsch

Merksatz:

Falscher Dienst bedeutet oft:
DNS,
NAT
oder Reverse Proxy falsch.

Fehlerbild: HTTPS zeigt falsches Zertifikat

Mögliche Ursachen:

- DNS zeigt auf falsche öffentliche IP
- Portweiterleitung zeigt auf falschen Server
- Reverse Proxy liefert falsches Zertifikat
- Hostname passt nicht
- falscher virtueller Host
- internes und externes DNS unterscheiden sich falsch

Merksatz:

Falsches Zertifikat kann durch falsches NAT oder DNS entstehen.

NAT und Dokumentation

NAT-Regeln sollten dokumentiert werden.

Wichtige Angaben:

- öffentliche IP
- externer Port
- internes Ziel
- interner Port
- Protokoll

- Zweck
- Verantwortlicher
- Datum
- Sicherheitsbewertung
- zugehörige Firewall-Regel
- DNS-Name
- Zertifikat

Merksatz:

NAT-Regeln ohne Dokumentation werden schnell unübersichtlich.

Typische NAT-Dokumentation

Beispiel:

DNS-Name	extern	intern	Zweck
wiki.firma.de	WAN TCP 443	192.168.10.20 TCP 443	Wiki
vpn.firma.de	WAN UDP 51820	192.168.10.5 UDP 51820	VPN
mail.firma.de	WAN TCP 25	192.168.20.10 TCP 25	Mail

Merksatz:

DNS,
externer Port,
internes Ziel
und Zweck zusammen dokumentieren.

NAT und Sicherheit prüfen

Regelmäßige Prüfung:

Welche Ports sind öffentlich offen?
Werden alle Weiterleitungen noch benötigt?
Sind die Zielsysteme aktuell?
Gibt es alte Testregeln?
Sind Adminoberflächen öffentlich?
Sind Quellbeschränkungen möglich?

Wird TLS genutzt?

Gibt es Logs?

Gibt es Monitoring?

Ist ein VPN besser?

Merksatz:

> Öffentlich erreichbare Dienste regelmäßig prüfen.

Was NAT nicht macht

NAT macht nicht automatisch:

- Dienst sicher
- Benutzer authentifizieren
- Schwachstellen schließen
- TLS einrichten
- Firewall-Regeln ersetzen
- DNS korrekt setzen
- Zertifikate passend machen
- Logs auswerten
- Angriffe verhindern

Merksatz:

> NAT ist Adressübersetzung,
> kein vollständiger Schutz.

Einordnung in das OSI-Modell

Thema	Schicht
NAT	3 / 4
PAT	3 / 4
Source NAT	3 / 4
Destination NAT	3 / 4
Portweiterleitung	3 / 4

Thema	Schicht
IP-Adresse	3
Port	4
Firewall-Regel	3 / 4 / je nach Firewall auch 7
DNS-Name	7
HTTPS-Zertifikat	6 / 7
Reverse Proxy	7

Merksatz:

> NAT betrifft IP-Adressen und Ports,
> also vor allem Schicht 3 und 4.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Was bedeutet NAT?
- Warum wird NAT bei IPv4 verwendet?
- Was ist PAT?
- Was ist der Unterschied zwischen NAT und PAT?
- Was ist Source NAT?
- Was ist Destination NAT?
- Was ist eine Portweiterleitung?
- Warum reicht NAT allein nicht als Firewall?
- Warum braucht man zusätzlich Firewall-Regeln?
- Was ist Hairpin NAT?
- Was ist Split DNS?
- Was ist CGNAT?
- Warum funktioniert eine Portweiterleitung bei CGNAT oft nicht?
- Warum kann Double NAT Probleme verursachen?
- Warum sollte man RDP oder SMB nicht direkt weiterleiten?
- Wie prüft man eine nicht funktionierende Portweiterleitung?

Typische Prüfungsfallen

NAT ist nicht Firewall.

Firewall ist nicht NAT.

NAT übersetzt IP-Adressen.

PAT übersetzt IP-Adressen und Ports.

Source NAT ändert die Quelle.

Destination NAT ändert das Ziel.

Portweiterleitung ist Destination NAT.

Private IPv4-Adressen sind nicht direkt im Internet geroutet.

Portweiterleitung macht interne Dienste extern erreichbar.

NAT-Regel allein reicht nicht,
wenn Firewall blockiert.

Firewall-Regel allein reicht nicht,
wenn NAT fehlt.

DNS muss auf die richtige öffentliche IP zeigen.

HTTPS braucht passendes Zertifikat.

Ein öffentlicher Port auf einer IP kann nur eindeutig weitergeleitet werden.

Reverse Proxy kann mehrere Webdienste über einen Port bündeln.

CGNAT verhindert oft eingehende IPv4-Verbindungen.

Double NAT erschwert Portweiterleitungen.

Hairpin NAT betrifft interne Clients mit öffentlicher Adresse.

Split DNS kann Hairpin NAT vermeiden.

NAT ist keine vollständige Sicherheitsmaßnahme.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
NAT	Network Address Translation
PAT	Port Address Translation
Source NAT	Quelladresse wird übersetzt
Destination NAT	Zieladresse wird übersetzt
Portweiterleitung	externer Port wird an internes Ziel weitergeleitet
private IP-Adresse	interne nicht öffentlich geroutete Adresse
öffentliche IP-Adresse	im Internet routbare Adresse
NAT-Tabelle	Zuordnung interner und externer Verbindungen
Hairpin NAT	interner Zugriff über öffentliche Adresse
NAT Loopback	anderer Begriff für Hairpin NAT
Split DNS	intern und extern unterschiedliche DNS-Antwort
CGNAT	Provider-NAT für mehrere Kunden
Double NAT	zwei NAT-Geräte hintereinander
Reverse Proxy	leitet Anfragen anhand von Hostnamen weiter
WAN-Port	externer Port auf öffentlicher Seite
interner Port	Port auf dem internen Zielsystem
Quellport	Port des sendenden Systems
Zielport	Port des Ziel-Dienstes

IHK-sichere Kurzformulierung

NAT steht für Network Address Translation und übersetzt IP-Adressen, häufig private IPv4-Adressen in eine öffentliche IPv4-Adresse. PAT steht für Port Address Translation und übersetzt zusätzlich Ports, damit mehrere interne Geräte gleichzeitig eine öffentliche Adresse nutzen können. Source NAT ändert die Quelladresse und wird typischerweise für ausgehenden Internetverkehr verwendet. Destination NAT ändert die Zieladresse und wird häufig für Portweiterleitungen genutzt. Eine Portweiterleitung macht einen internen Dienst von außen erreichbar, benötigt aber neben der NAT-Regel auch passende Firewall-Regeln, einen laufenden Dienst, korrekte DNS-Einträge und bei HTTPS ein passendes Zertifikat. NAT ist keine vollständige Sicherheitsmaßnahme und ersetzt keine Firewall.

Merksätze

NAT = Network Address Translation.

PAT = Port Address Translation.

NAT übersetzt IP-Adressen.

PAT übersetzt IP-Adressen und Ports.

Source NAT ändert Quelle.

Destination NAT ändert Ziel.

Portweiterleitung ist Destination NAT.

Private IPv4-Adressen sind intern.

Öffentliche IPv4-Adressen sind im Internet routbar.

NAT ermöglicht Internetzugang mit privaten IPv4-Adressen.

PAT ermöglicht viele Clients über eine öffentliche IP.

NAT-Tabelle merkt sich Zuordnungen.

NAT ist keine Firewall.

Firewall ist kein NAT.

NAT-Regel und Firewall-Regel müssen zusammenpassen.

Portweiterleitung erhöht die Angriffsfläche.

Admin-Dienste nicht direkt ins Internet öffnen.

RDP nicht direkt weiterleiten.

SMB nicht direkt weiterleiten.

SFTP oder VPN sicherer als unverschlüsseltes FTP.

Reverse Proxy bündelt Webdienste.

DNS muss zur öffentlichen IP passen.

Zertifikat muss zum Hostnamen passen.

CGNAT verhindert oft eingehende IPv4-Verbindungen.

Double NAT erschwert Portweiterleitungen.

Hairpin NAT = intern über öffentliche Adresse.

Split DNS liefert intern andere Antworten.

NAT braucht passenden Rückweg.

NAT ersetzt kein Sicherheitskonzept.